Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of		
	)	
Downloadable Security Technology Advisory Committee (DSTAC)	)	MB Docket No. 15-64
	)	

COMMENTS OF VERIMATRIX, INC.

Tom Munro, Chief Executive Officer, and

Petr Peterka, Chief Technology Officer

Verimatrix, Inc..
6059 Cornerstone Ct W,
San Diego, CA 92121
(858) 677-7800

Dated: October 7, 2015

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of		
	)	
Downloadable Security Technology Advisory	)	MB Docket No. 15-64
Committee (DSTAC)	)	

COMMENTS OF VERIMATRIX, INC.

Verimatrix, Inc. (“Verimatrix”) hereby submits these comments in response to the Media Bureau's Public Notice seeking comment on the DSTAC report.

I. INTRODUCTION

Verimatrix is the world's leading IPTV security provider and also provides security to the broader content distribution community including satellite, cable and broadband. Overall, we serve more than 800 PayTV operators around the world and protect more than 78 million screens with our Conditional Access (CA) and Digital Rights Management (DRM) systems. In the United States, we are the security provider for more than 100 telephony and cable-based Multi-channel Video Program Distributors (MVPDs) with more than 1 million subscribers. As such, Verimatrix sought membership on the DSTAC committee, but was not invited to participate. Nonetheless, Verimatrix attended every public DSTAC meeting, was invited to DSTAC working group meetings to provide security expertise, and provided expertise to the members whenever permitted to do so under the rules of the process. With this expertise and background in the proceedings, we offer these comments on the resulting DSTAC report.

II. SUMMARY OF COMMENTS

In response to the demands of our customers, Verimatrix has solved the security aspects of a problem very similar to the problem presented to DSTAC. Our solution supports multiple DRMs using downloadable software; however, our goal was not "DRM unification" but instead "user rights unification" to enable transparent content consumption for the end-users across a variety of navigation devices. The two proposals outlined in the DSTAC report can be used as part of Verimatrix's solution, but neither forms the basis for the totality of the security system that we provide to the MVPDs, or even the preferred path to reach the increasingly broad range of client devices upon which consumers watch and enjoy the services.

In its work, the DSTAC committee rather quickly decided not to propose the standardization of a single "downloadable security" system. We agree with this conclusion since we believe that such an approach would be harmful to competition, innovation and security as we will explain further in these comments.

Regarding the specific proposals in the reports of DSTAC Working Groups 3 and 4, we ask the Commission not to mandate either or even both as "the" standard solution. We view the two proposals, and their various combinations, as useful alternatives as part of a toolkit of approaches. However, each proposed system has deficiencies that preclude it from being suitable as a total solution. Through our current solution, Verimatrix offers a variety of options to its customers, including those options represented by the two proposals, but we do not envision any reasonably complex or robust PayTV system relying exclusively on either or even both of these alternatives.

Returning to the original question of "downloadable security" put before the DSTAC, we reiterate that we do not favor forced standardization by government mandate at this level. However, certain discrete elements and interfaces within an MVPDs security system can be standardized on a go-forward basis that would be helpful to competition and innovation without undue harm to security. We have these interfaces clearly identified in our solutions and are working on voluntary standardization of them in various fora. We will highlight these possible areas of standardization herein, but we do not propose that the FCC mandate them.

III. VERIMATRIX HAS SOLVED A PROBLEM VERY SIMILAR TO THE PROBLEM PRESENTED TO DSTAC USING AN APPROACH DIFFERENT FROM THE PROPOSALS IN THE DSTAC REPORT

In order to respond to the demands of our customers, Verimatrix has had to solve a problem very similar to the problem presented to DSTAC. We have a diverse set of PayTV operators that use managed satellite, cable and IPTV systems, sometimes in combination with unmanaged over-the-top services (OTT) to reach consumers using both operator-provided STBs and consumer-owned retail devices such as tablets and smart TVs. Our customers also include both greenfield and legacy systems. To meet this need that parallels the DSTAC problem rather closely, we developed a system that we call Video Content Authority System (VCAS™). The first stage of VCAS involves the portion of the system that is under total control of the operator, both in the head-end and on the consumer side through total control of the security of the receiver, e.g., set-top box, which include what we call ViewRight® clients. The problem then is how does one extend the PayTV operator's services to all of the other devices that consumers increasingly wish to use to enjoy television and other accompanying services. Verimatrix accomplishes this with an extension to VCAS that we call MultiRights™. MultiRights brings CE devices and HTML5 browsers with embedded, non-Verimatrix clients under the VCAS unified revenue security umbrella together with other subscriber devices already incorporating the ViewRight clients. The goal is not "DRM unification" as much as user rights unification to enable transparent and consistent content consumption for the end-users.

The MultiRights framework allows for the inclusion of any third-party DRM scheme and client devices under the VCAS umbrella for complete end-to-end management of revenue security, which includes content security. MultiRights provides server-side support for secure content distribution to STBs, PCs, and off-the-shelf consumer electronics and mobile devices, when equipped with compatible media players and native DRM clients. No DRM is required to support all consumer devices. No consumer device is required to support all DRMs. A unified security management system in the head-end supports several DRMs allowing it to connect to a wide range of consumer devices. The two proposals outlined in the DSTAC report can be used as part of this, but neither forms the basis for the totality of the security system provided to the MVPDs, or even the preferred path to reach the increasingly broad range of client devices upon which consumers watch and enjoy the services.

Verimatrix does not propose that the FCC mandate our system or approach. We merely seek the opportunity to compete and offer our rich security infrastructure that enables an equally rich and powerful PayTV system that meets the revenue protection needs of the PayTV operator, the content protection demands of the content provider, and the constant innovation and ease of use needs of a demanding consumer base. If the Commission were to mandate either of the proposals included in the DSTAC report, then we are concerned that the US PayTV market will continue to be segregated from and uncompetitive with innovative and successful platforms developed in other markets. And, the thriving competitive market being catalyzed by the rapid adoption of internet technologies might instead by frozen in place.

IV. STANDARDIZATION OF A SINGLE DOWNLOADABLE SECURITY SOLUTION WOULD BE HARMFUL TO COMPETITION, INNOVATION AND SECURITY

There have been numerous attempts in the past to standardize security and all have faced one intractable problem - they create single points of attack. Diversity is an important aspect of security - if one system falls, it doesn't necessarily impact the other systems. The urge to standardize and the benefits therefrom have nonetheless driven many activities to standardize certain aspects of security systems. The PayTV industry has had certain success in standardizing: i) common encryption and scrambling algorithms; ii) simulcrypt broadcast architectures; iii) entitlement message formats; iv) usage rights message formats; v) certificate formats; vi) key ladder functionality for chips; and other similar components of a security system. However, the industry is very careful in any such endeavor to avoid the trap of a single point of failure.

Further, there is vibrant competition and innovation among security providers alongside the competition and innovation among the traditional PayTV providers, over-the-top providers and consumer device providers. While all can benefit from standardization, premature or unwise standardization, especially when locked-in through government mandate, can stifle innovation and competition in all areas except those "allowed" by the standard. For example, the CableCARD created some benefit through its standardization, as evidenced by the consumer products that use it; however, the very definition of that standard forced all competition and innovation to stay within the bounds of what the CableCARD allowed and disallowed.

Another aspect of security standardization is assigning responsibility for the overall security of the system. If secured content distribution business models are to be successful in the long term, there must be contingency plans for what to do when things go wrong. Certain PayTV operators have had to do smartcard swap-outs, box swap-outs or full system upgrades in the past. These are costly endeavors that go beyond the typical limitation of liability clauses of common 3rd party content protection licenses. The use of software downloadable solutions does not completely insulate one from these costs, since the software must be downloaded into a secure hardware environment that is also subject to attack. The PayTV provider and its security provider typically determine in their bi-lateral agreements who will do what when things go wrong. Any successful security standard inserted into the PayTV pathway must address this problem.

Forced standardization suffers the risk of missing the mark and stifling innovation. Forced standardization in security areas suffers the risk of being broken and harming the very markets it intended to facilitate.

V. EACH PROPOSED SYSTEM HAS DEFICIENCIES THAT PRECLUDE IT FROM BEING SUITABLE AS A TOTAL SOLUTION

A. Link Protection, such as DTCP-IP, was not proposed by DSTAC as a one-size-fits-all solution, nor is it suitable as such

The "Virtual Headend System" proposal recommends performing the operator controlled security such as network security, Conditional Access (CA) and Digital Rights Management (DRM) "in the cloud", and then passing control to a link protection mechanism such as DTCP-IP to interface to retail devices. Link protection is useful for protecting content in certain situations, e.g., passing content from point A to point B, but it lacks the richness of business model support and persistent protection of a DRM. Verimatrix's customers pass content from our system to link protection systems like DTCP-IP and HDCP regularly, but never as the sole available path to their customer's navigation devices. Link protection is an important tool, but was not proposed by DSTAC as a one-size-fits-all solution, nor is it suitable as such.

B. The Application Model, through HTML-5 Encrypted Media Extensions, was not proposed by DSTAC as a one-size-fits-all solution, nor is it suitable as such

The "HTML5 Security APIs" proposal recommends that operators use a non-exclusive security interface to consumer electronics devices, specifically highlighting HTML5 with Encrypted Media Extensions (EME). HTML5 and EME are important tools to gain broad reach to devices with browsers or subsets thereof, but they are missing the actual downloadability component. Furthermore, they are typically limited to PC browsers – in fact, binding proprietary DRM solutions to proprietary browsers - and not as applicable to applications that do not use HTML as the user interface language. Verimatrix's uses HTML5 and EME to help our customers reach many of their customer's devices, but never as the sole available path. HTML5 EME is an important tool, but was not proposed by DSTAC or the HTML5 Security APIs proposal authors as a one-size-fits-all solution, nor is it suitable as such.

VI. STANDARDIZATION OF CERTAIN ELEMENTS OF MVPD SECURITY SYSTEMS WOULD BE HELPFUL TO COMPETITION AND INNOVATION WITHOUT UNDUE RISK TO SECURITY

Regarding the original question of "downloadable security" put before the DSTAC, we reiterate that we do not favor forced standardization by government mandate in this area. However, certain discrete elements and interfaces within an MVPDs security system can be standardized on a go-forward basis that would be helpful to competition and innovation without undue harm to security. Possible areas of standardization include:

a) CAS Client interfaces in common platforms such as RDK, Android TV, etc.

b) Client device HW Abstraction API (e.g., SCTE OMS K-LAD)

c) CAS metadata containers (e.g., MPEG-2 TS, MPEG-DASH, HLS, etc.)

d) Content format and encryption (NIST AES-128, MPEG CENC, etc.)

e) Secure OS and downloadability (e.g., GlobalPlatform Trusted Execution Environment (TEE))

However, under no circumstances can we foresee recommending standardization of:

a) CAS system (authentication, key management, etc.)

b) SW/HW hardening (obfuscation, key derivation, etc.)

We have these interfaces clearly identified in our solutions and are working on voluntary standardization of certain appropriate interfaces in various fora. We highlight these possible areas of standardization for completeness with respect to the "downloadable security" question, but we do not propose that the FCC mandate them.

VII. CONCLUSION

We reiterate our agreement with the DSTAC report that there is no one-size-fits-all solution to reach the navigation devices of consumers. We also agree that it should not be necessary to disturb the present and future CA/DRM choices made by MVPDs. Verimatrix and other vendors already offer solutions that achieve "user rights unification" and enable transparent content consumption for the end-users across a variety of navigation devices. The two proposals outlined in the DSTAC report are used as part of Verimatrix's solution, but neither is sufficient to the rapidly changing, voracious consumer appetite for content on an increasingly diverse set of navigation devices.

Respectfully submitted,

By: ________________________

Tom Munro
Chief Executive Officer

Verimatrix, Inc..
6059 Cornerstone Ct W,
San Diego, CA 92121
(858) 677-7800

By: ________________________

Petr Peterka
Chief Technology Officer

Verimatrix, Inc..
6059 Cornerstone Ct W,
San Diego, CA 92121
(858) 677-7800

October 7, 2015